The Rising Threat to CEOs: Lessons from World Security Report 2025

Prepared by Warren Pulley – CrisisWire Threat Management Solutions

■ crisiswire@proton.me | ■ https://rypulmedia.wixsite.com/crisiswire

Introduction

The World Security Report 2025 highlights a stark reality:
CEOs and senior executives are now among the most targeted individuals worldwide.
From cyber-enabled doxxing to geopolitical risks and insider threats, leaders face unprecedented dangers.
This report is not just about statistics — it is a warning signal for boards and security leaders.

Key Findings from the Report

- **74% of CEOs** reported increased security concerns in 2025.
- **Insider threats** and employee-driven risks rank as the fastest-growing category.
- **Cyber-physical convergence** has made digital leaks into physical threats.
- **Geopolitical instability** creates new risks for multinational leadership travel.

Why CEOs Are at Greater Risk

- **Visibility:** CEOs are public figures, often with accessible digital footprints.
- **Polarization:** Social and political divisions amplify targeting.
- **Hybrid Work:** Remote access has widened the attack surface.
- **Personal Branding:** Many CEOs are influencers, attracting both admiration and hostility.

Case Studies

- **Targeted:** A European CEO was harassed and stalked after personal data leaked online.
- **Attack:** An Asian energy executive was targeted during geopolitical unrest tied to company operations.
- **Prevented:** A U.S. CEO’s travel risk was mitigated by pre-deployment intelligence and protective planning.

These cases show the difference between reactive and proactive executive security.

Leadership Responsibility

Boards and CEOs cannot treat executive protection as a “perk.”
It is an operational necessity. Liability now extends to governance:
- Failure to protect executives can be deemed negligence.
- Investors increasingly question leadership resilience and continuity.
- Insurers require executive protection policies for coverage in high-risk sectors.

Actionable Steps for CEOs & Boards

1. Conduct annual executive threat assessments (cyber + physical).
2. Align with ASIS Executive Protection Standard (2025).
3. Invest in insider threat detection programs.
4. Develop global travel security protocols.
5. Train executives in personal digital hygiene and resilience.

Resources & Backlinks

- CrisisWire Blog Hub: https://rypulmedia.wixsite.com/crisiswire/blog
- Services: https://rypulmedia.wixsite.com/crisiswire/services
- Reddit Hub: https://www.reddit.com/user/crisiswire/m/rcrisiswireassessments/
- Book: The Prepared Leader (Amazon) https://www.amazon.com/dp/B0FS1D2KS3
- World Security Report 2025:
https://www.allianz.com/en/press/news/2025/world-security-report.html
- ASIS Executive Protection Standard: https://www.asisonline.org

Call to Action

Executives are more exposed than ever.
The question is not whether threats exist — but whether leadership is prepared.

■ crisiswire@proton.me
■ https://rypulmedia.wixsite.com/crisiswire

FAQ

Q: Why are CEOs targeted more now than before?
A: Increased digital footprints, polarization, and geopolitical instability make them vulnerable.

Q: What is the World Security Report 2025?
A: A global survey highlighting key risk trends for leaders and organizations.

Q: How can CEOs reduce their risk?
A: By aligning executive protection programs with ASIS standards and conducting annual audits.

Q: Are insider threats a major risk to executives?
A: Yes, employees and contractors often have privileged access that can be exploited.

Q: What role should boards play?

A: Oversight and funding of executive protection programs, ensuring resilience and continuity.